UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,525	01/25/2001	Michael Hrabik	881075/3	5856

7590 09/15/2003

Joel E. Lutzker, Esq.
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/770,525	HRABIK ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-22 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3, 5-6, 11, 13, 15, 17, 19, 21-22 are sill rejected under 35 U.S.C. 103(a) as being unpatentable over (Messmer and Newton's Telecom Dictionary).

3. As per claims above, Messmer teaches outsourcing intrusion detection. Messmer also teaches that Counterpane manages intrusion-detection services, by having a black box that is located on a companies network. Thus, the Examiner asserts that by having the black box sensor that is located on the network, this constitutes a security subsystem, because the security subsystem continuously monitors and collects data and transmits the information to Counterpane's data center(i.e. Master system). Also, because the Applicant provides no specific definition of a master system, the Examiner broadly interprets a master system to be any system that is analyzes information from the subsystem, because Messmer teaches that all data from customer's network is transmitted to the Master system(i.e. Counterpane's data center). Further, Messmer teaches that the subsystem(i.e. black box) is configured to correlate events across a plurality of devices associated with the network of computers and detect attacks on the computer, because Messmer teaches that a probe or "black box sensor" is put on the customer's network(i.e. target network) to accept audit data from a wide range of devices. Further, Messmer teaches that the black box sensor captures syslog and audit outputs from Windows NT, Solaris,

Linux servers; firewalls; ISS and intrusion detection software. Further, master system(i.e. Counterpane's data center) registers information pertaining to attacks detected by the security subsystem(i.e. black box), because Messmer teaches that the black box regularly transmits the network activity output to the master system(i.e. data centers). Furthermore, Messmer teaches that the data that is transmitted to the master system(i.e. data center) are footprints of attacks, and the data center has analysts that are trained to understand them. Thus, the Examiner asserts that the data that is transmitted is outputted to the master system(i.e. data center), and registered so the information can be analyzed by the analysts. Lastly, Messmer teaches that the security subsystem(i.e. black box) and the master system(i.e. Counterpane's data center) communicates by using encryption, because Messmer teaches that the Counterpane's black box regularly transmits the network activity output in encrypted form to Counterpane's data center(i.e. master system).

4. The Examiner asserts that since the Applicant does not provide a definition of a secure link(i.e. channel). The Examiner looks towards Newton's Telecom Dictionary. According to Newton's Telecom Dictionary, a secure channel(i.e. link) is defined as technology that provides privacy, integrity, and authentication in point-to-point communication(see pg. 636). Thus, the Examiner asserts that the encryption taught in Messmer is a secure channel, because encrypting insures that information is protected from unauthorized viewing or use; therefore, insuring privacy, and integrity is maintained because if information is private the information cannot be manipulated, and authentication because in encryption in order to decode the information one must have the corresponding key to decode. Thus, the motivation to have an encrypted channel(i.e. link) is that the information that is sent between the two points of security subsystem

and the master system is kept private and integrity is kept, and both parties can be authenticated, and thus prevents intruders or unauthorized users from manipulating information.

5. As per independent claims 11, 21-22, and also dependent claims 3, 6, 15, 19, limitations have already been addressed see claim 1 above. Also, claims 11, 21-22, 3, 6, 15, 19 include a master system hierarchically independent from the security subsystem. The Examiner asserts that Messmer discloses this because Messmer teaches that the master system(i.e. data center) is located in California or Virginia and that all data located on customer's network is transmitted to the master system. Also, the master system monitors the security subsystem around the clock, and the master system and Messmer also teaches that the master system is an outsourced intrusion detection. Thus, the Examiner asserts that the Master system is hierarchically independent from the security subsystem.

6. As per claims 4, 7, Messmer teaches that a security subsystem is hierarchically subordinate to the master system, because Messmer teaches that the customer's network has a black box sensor that correlates all the information from devices on the customer's network(see claim 1, above), and this information is transferred to the Master system. Further, the master system(i.e. data center) of Messmer tells customer's how to handle intrusion's. Therefore, the Examiner asserts that the security subsystem is subordinate to the master system.

7. As per claims 14, 18, Messmer teaches that the detection means(i.e. black box sensor) is one or more selected from the group consisting of an intrusion detection system, firewall and security subsystem. The Examiner asserts that Messmer meets this limitation, because the black box sensor detects attack on the network.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2, 8, 12, 16, 20 are still rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer and Newton's Telecom Dictionary, in view of Kurtzberg et al. and further in view of Hill et al.

10. As per the claims above, Messmer is silent on how the data center test for vulnerabilities. However, Kurtzberg et al. discloses testing a system by having a psuedo(i.e. simulated) attack generator for generating attacks on the computer(see col. 3, lines 21-28). Although, Messmer does not explicitly disclose comparing pseudo-attack to the attacks detected by the security subsystem, the Examiner looks towards Hill et al. for this feature. Hill et al. discloses comparing pseudo-attacks(i.e. training attacks) to the attacks detected by the security system(see col. 3, lines 20-36).

11. It would have been obvious to modify Messmer and Newton's Telecom Dictionary with the features of Kurtzberg et al. and Hill et al. The Messmer and Newton Dictionary do not teach how the testing is done. Therefore, the Examiner looks towards Kurtzberg et al. and Hill et al. to include the features of pseudo attack generator and comparing the psuedo attacks to attacks detected by the system. Thus, the motivation to include how the testing is performed of Kurtzberg and Hill et al. with Messmer and Newton's Telecom Dictionary combination includes the data center testing for vulnerabilities of the security subsystem by using the pseudo attack

generator, and comparing the pseudo attacks to attacks detected by the system. This method of testing insures that integrity is maintained by testing the security subsystem thereby protecting the network form unauthorized penetrations(see col. 1, lines 35-40 of Kurtzberg et al.). Thus, integrity of a computer system can be tested reliably to improve or complement the system performance(see col. 1, lines 65-67 of Kurtzberg).

12. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer and Newton Telecom Dictionary, Kurtzberg and further in view of Hill as applied to claim 8 above.

13. As per claim 9, the Examiner asserts that Messmer discloses this because Messmer teaches that the master system(i.e. data center) is located in California or Virginia and that all data located on customer's network is transmitted to the master system. Also, the master system monitors the security subsystem around the clock, and the master system and Messmer also teaches that the master system is an outsourced intrusion detection. Thus, the Examiner asserts that the Master system is hierarchically independent from the security subsystem.

14. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer and Newton Telecom Dictionary, Kurtzberg and further in view of Hill as applied to claim 8 above.

15. As per claim 10, Messmer teaches that a security subsystem is hierarchically subordinate to the master system, because Messmer teaches that the customer's network has a black box sensor that correlates all the information from devices on the customer's network(see claim 1, above), and this information is transferred to the Master system. Further, the master system(i.e. data center) of Messmer tells customer's how to handle intrusion's. Therefore, the Examiner asserts that the security subsystem is subordinate to the master system.

Response To Amendment

16. In regards to Applicant's remarks that the previous office action was improperly made final. The previous office action was not made final, the previous office action contained no such paragraph stating that the office action has been made final. On the office action summary of the previous rejection, the Examiner inadvertently checked the wrong box made final. The previous office action was non-final, there was no such paragraph stating that it was final. This rejection is now final, please see below for the paragraph, in bold that states Final Rejection. The Applicant is also, urged to look at MPEP 710.06, situations for when the reply period is restarted, where there is a citation of a reference incorrect, or an office action defect, and when this error is called to the attention within the statutory period the period will be restarted. The Examiner asserts that neither situations apply in regards, to restarting the period.

17. Second, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the feature upon which applicant relies (i.e., correlate) was not defined with this specific definition. If the Applicant wishes to claim a specific definition of correlate it must be claimed. Also, Messmer does teach correlate events across a plurality of devices associated with the network of computers and to detect attacks on the computer(see previous rejection, pg 2). Thirdly, the Examiner is to interpret the claims broadly. Fourthly, the Applicant states that correlation was discussed in the interview on March 12, 2003. The Examiner, Attorney, and Applicant discussed the invention, and the prior art that was used in office action dated July 2, 2002, and more specifically, discussed "monitoring the network in its entirety".

18. The Applicant states that Messmer teaches that the entire analysis of the captured and transmitted data is performed at the operating center, not the black box. Further, the Applicant states that the black box only captures the security-related data and passes it onto the data center. The Examiner disagrees that Messmer does not only teach the black box captures the security-related data and passes it onto the data center, but also the black box senses attacks occurring in the system, and the data that is collected by the black box, contains the footprints of attacks. Therefore, the Examiner asserts that the subsystem detects attacks, because the data that is correlated has footprints of attacks in the data. Therefore, Messmer not only teaches the operating center analyzes the data, but also the subsystem detects attacks, and the operating center advise companies how to combat threats. The Applicant also states that the analysis of attacks is not automated. The Examiner asserts that this feature is not claimed.

19. For the following reasons above, the claimed invention is not allowable, and the prior art that was used previously is still rejected under the claims. Therefore, this action is Final, see Final paragraph below.

20. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

***

August 28, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100